IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Paul Gassoway
Serial No.:	10/849,318
Filing Date:	May 19, 2004
Group Art Unit:	2136
Examiner:	Oscar A. Louie
Confirmation No.	5789
Title:	**Method and Systems for Computer Security**

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

PRE-APPEAL BRIEF REQUEST FOR REVIEW

The following Pre-Appeal Brief Request for Review ("Request") is being filed in accordance with the provisions set forth in the Official Gazette Notice of July 12, 2005 ("OG Notice"). Pursuant to the OG Notice, this Request is being filed concurrently with a Notice of Appeal. Applicant respectfully requests reconsideration of the application in light of the remarks set forth below.

REMARKS

Applicant received a Final Office Action dated February 22, 2008 ("Office Action") to which Applicant responded with a response dated April 22, 2008 ("Previous Response"), after which, Applicant received an Advisory Action dated May 20, 2008 ("Advisory Action"). At the time of the Advisory Action, Claims 1-24 were pending, of which, Claims 1-24 were rejected. Applicant seeks review of the rejections of Claims 3, 6, 9, 12, 15, 18, 21 and 24. Applicant does not seek review in this Request of the rejections of Claims 1-2, 4-5, 7-8, 10-11, 13-14, 16-17, 19-20, and 22-23.

Claim Rejections - 35 U.S.C. § 103

The Examiner rejects Claims 3, 6, 9, 12, 15, 18, 21, and 24 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,279,113 to Vaidya ("*Vaidya*") in view of U.S. Patent No. 7,032,114 to Moran ("*Moran*"). Applicant respectfully traverses these rejections for the reasons discussed below.

Claim 3, which depends from independent Claim 1, discloses a method for maintaining security of a computer system. The method includes the steps of comparing received data with a database of signatures, increasing a system certainty value if the received data does not match a signature in the database, and decreasing the system certainty value if the received data matches a signature in the database. Claim 3 further discloses that the increased or decreased certainty value becomes the initial system value.

First of all, the Examiner admits that *Vaidya* fails to explicitly disclose either increasing or decreasing the system certainty value. *Office Action*, pg. 4. Instead, the Examiner claims that the timer/counter based attack signature profile of *Vaidya* suggests these limitations "for the purposes of determining whether a particular event has occurred a threshold number of times." *Office Action*, pg. 5. Applicant respectfully contends that the limitations of increasing and decreasing the system certainty value do not merely determine whether a particular event has occurred a threshold number of times.

Furthermore, the Examiner states that *Vaidya* suggests that "the threshold may be set/selected accordingly/being adjustable (i.e. increased/decreased)." *Advisory Action*, pg. 2. Applicant respectfully points out that *Vaidya* discloses a "preselected threshold." *Vaidya*, col. 4, line 26 (emphasis added). Applicant respectfully contends that this preselection fails to disclose, teach, or suggest the threshold being adjustable after comparing the received data with a database of signatures. Additionally, when the timer/counter attack signature profile is used, *Vaidya* discloses that no action is taken when an incoming expression fails to match the signature. *See Vaidya*, col. 12, lines 23-26. Applicant respectfully contends that the Examiner's use of suggestions within suggestions appears to be reliance on hindsight to recreate the limitations of Claim 1. "However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art." M.P.E.P. § 2142. Therefore, Applicant respectfully contends that *Vaidya* fails to disclose the limitations "increasing the system certainty value if the received data does not match a signature in the database" and "decreasing the system certainty value if the received data matches a signature in the database." *Moran* fails to cure this deficiency. Accordingly, Applicant respectfully contends that Claim 3 is patentably distinguishable from the references cited by the Examiner.

Claim 3 further discloses that the increased or decreased certainty value becomes the initial system value. The Examiner states that *Moran* makes these limitations obvious for "purposes of readjusting the threshold to reduce the possibility of a false positive." *Office Action*, pg. 8. However, the cited portion of *Moran* discloses that false positives are reduced by using a "broader range of information," such as information about past intrusions or suspicious events from other platforms. *See Moran*, col. 8, lines 1-6, 26-42. This broader range of information allows the alert threshold of *Moran* to be set higher. *Moran*, col. 8, lines 40-42. Applicant respectfully contends that this use of a broader range of information and an alert threshold that is set higher fail to disclose, teach, or suggest "the increased or decreased certainty value becomes the initial system value." For at least these reasons, Applicant respectfully contends that Claim 3 is patentably distinguishable from the proposed *Vaidya-Moran* combination. Claims 9, 15, and 21 are patentably distinguishable for analogous reasons.

Claim 6 depends from Claim 1 and incorporates all the limitations thereof. As shown above, the proposed *Vaidya-Moran* combination fails to disclose, teach, or suggest increasing the system certainty value or decreasing the system certainty value. For at least these reasons, Applicant respectfully contends that Claim 6 is patentably distinguishable from the references cited by the Examiner.

Furthermore, Claim 6 discloses that the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded. The Examiner admits that *Vaidya* fails to disclose this limitation and relies instead on *Moran*. However, the cited portion discloses "a mechanism for checking timestamps, configured to identify backward and forward time steps in a log file." *Moran*, col. 4, lines 28-31. While this discloses identifying time steps in a log file, *Moran* fails to disclose, teach, or suggest actually generating a log file. Furthermore, there is no disclosure, teaching, or suggestion in *Moran* that the log file indicates that data matching a signature was forwarded. Accordingly, Applicant respectfully contends that Claim 6 is patentably distinguishable from the proposed *Vaidya-Moran* combination. Claims 12, 18, and 24 are patentably distinguishable for analogous reasons.

Conclusion

As the rejections of Claims 3, 6, 9, 12, 15, 18, 21 and 24 contain clear legal and factual deficiencies, Applicant respectfully requests a finding of allowance of Claims 3, 6, 9, 12, 15, 18, 21 and 24. If the PTO determines that an interview is appropriate, Applicant would appreciate the opportunity to participate in such an interview. To the extent necessary, the Commissioner is hereby authorized to charge any required fees or credit any overpayments to Deposit Account No. **02-0384** of **Baker Botts L.L.P.**

Respectfully submitted,
BAKER BOTTS L.L.P.
Attorneys for Applicants

Luke K. Pedersen
Reg. No. 45,003
Phone: (214) 953-6655

Date: 6-17-08

CORRESPONDENCE ADDRESS:

Customer Number: **05073**